DESIGN AND IMPLEMENTATION OF SMART DOOR LOCKED SYSTEM USING IoT HOME AUTOMATION

By:

OLOWU, BOLUWATIFE DAVID

HND/23/COM/FT/0111

Submitted to the

DEPARTMENT OF COMPUTER SCIENCE,

INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGY (IICT), KWARA STATE POLYTECHNIC, ILORIN

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN COMPUTER SCIENCE

JUNE, 2025

APPROVAL PAGE

This is to certify that this project was carried out by **OLOWU, BOLUWATIFE DAVID** with Matric Number: **HND/23/COM/FT/0111** has been read and approved by the Department of Computer Science, Kwara State Polytechnic Ilorin. In partial fulfillment of the requirements for the award of Higher National Diploma (HND) in Computer Science.

____________________ ____________________

Dr. Ayeni, J.K.
Project Supervisor ***Date***

____________________ ____________________

Mr. Oyedepo, F.S.
Head of Department ***Date***

____________________ ____________________

External Examiner ***Date***

DEDICATION

This research project is dedicated to the Almighty God, the giver of life and taker of life that guide me throughout my program.

ACKNOWLEDGEMENTS

All Glory and adoration belong to him alone (God), Omniscience, and Omnipresent for his mercy over me throughout my undergraduate journey, which of your favour will I deny absolutely none.

First and foremost, I would like to express my deepest gratitude to my project supervisor, in person of **Dr. Ayeni, J.K.** for his unwavering support, insightful advice, and constructive feedback throughout the development of this project.

Also, to my lovely parents, indeed I am speechless to thank you today, I pray to the Almighty Allah to grant you both all your heart desires. May you both live long to eat the fruit of your labour.

Also, to the school management (Kwara State Polytechnic, Ilorin) and entire Staff of Computer Science Department, starting from the Head of Department in person of **Mr. Oyedepo.** I appreciate you all.

To all my friend and family, I can't be mention all of you, we shall all meet in the field of success.

Thank you all.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The rapid advancement in technology has brought about a significant transformation in security systems, with smart door locks emerging as a reliable alternative to conventional locking mechanisms. This seminar report presents the design and implementation of a Smart Door Lock System integrated with an Automatic Intruder Alarm, aimed at enhancing the security of homes, offices, and restricted areas. The system employs a combination of microcontroller technology, sensors, and electronic control to ensure authorized access and real-time intrusion detection. Access control is managed using methods such as keypad input, RFID cards, or biometric authentication, depending on the chosen design. When an authorized user inputs the correct credentials, the microcontroller signals a servo motor to unlock the door. In contrast, any forced entry or unauthorized tampering triggers an intruder detection system, usually comprising a Passive Infrared (PIR) sensor or vibration sensor, which activates a buzzer or siren alarm to notify occupants of a security breach. For enhanced functionality, a GSM module can be included to send SMS alerts to the homeowner's mobile device. This project offers a practical solution to increasing security challenges by combining automation with real-time alert systems. It also demonstrates the potential of integrating Internet of Things (IoT) components into home security solutions. The system is cost-effective, user-friendly, and scalable, making it suitable for a wide range of applications. The project ultimately highlights how embedded systems and smart technologies can be utilized to develop efficient and intelligent security systems for modern living environments.

Keywords: Intruder, Internet of things, Trigger, Security & Smart Door Lock.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

The concept of home automation has been around since the late 1970s though with the advancement in technology and services, people's expectations of what a home should be or how the services should be provided for and accessed at home continues to change. Smart Home describes a residence that has appliances, lighting, heating, air conditioning, televisions, computers, entertainment (audio and video systems), security, and camera systems that can communicate with one another and can be controlled remotely by a time schedule, from any room in the home, as well as remotely from any location in the world by phone or internet facility.(Edmonds & Chandler, 2008).

Today, mobile phones are used as clocks, calendars or controllers instead of just for making and receiving calls. With the help of the internet, a mobile device can be used to implement a smart home by controlling devices and getting alerts. The Internet of Things (IoT) is a system of inter-related computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction, (Wadhwa & Puri, 2016). Now and over time efficient, convenient, and safe ways to access homes will be provided for. Irrespective of the change in user expectations, advancement of technology, or change of time, the role of a home automation system has remained the same. Throughout the late 1990s and early 2000s, smart technologies has emerged, with gadgets and devices becoming more and more common, and more affordable.

A home automation system uniquely solves all of the aforementioned problems. The home automation for many years was a customary science-fiction subject. A lot of movies and books reconnoitered in theory miscellaneous technologies for decades. Aside from, today we live in the world that empowers us to build a variety of automation systems without much difficulty as compared to just a couple of years back. Home automation is a concept of controlling and automating everyday tasks as well as needs. This process involves centralizing the control logic for various devices and electrical components in the house ranging from light bulbs to more sophisticated devices like heating/cooling units, windows, and doors (Ponte, 2016). The list of devices that fit in home automation sector is always growing. Gartner, a world leading information technology research company, noted that approximately 5 billion Internet of Things (IoT) devices were connected via internet in the year of 2015 without any others being included. Moreover, they predicted that about 25 billion devices will be connected by the year of 2020. It is fair to note that their prediction is among the lowest as compared to some others in the market (Rivera & Meulen, 2014). General idea of home automation is probably very old, however, first functional prototypes were started developing some half a century ago. Yet real progress in the industry has been made little over a decade back (Haddon, 1995). With the technological revolution in the early 2000s, many IoT devices emerged promising aid in normal tasks and regularly making our lives unhurried and relaxed. According to NPD Group in 2013, 93% of households in the USA were connected with internet and owned at least one personal computer. Around 60% households owned smart-phones and tablets All these numbers together with perpetually rising demand for new devices become a solid ground for home automation to be the following big thing. It is worth a mention that the European markets for home automation-based systems are a bit behind than North American markets (Kumar, 2014).

One of the smart phone applications that have been developed is smart homes technology (John et al., 2020). Smart home technology is the technologies that are used in homes with various apparatus converse over a local network. According to the Smart Homes Association the best definition of smart home technology is: the combination of technology and services through home networking for a better value of living. This technology can be used to monitor, alert and execute, according to the desired functions. Smart homes technology makes automatic connection with environment via Internet, telephone or regular fixed phones. Smart homes actually have the ability to make life easier and more proper. Home networking can also offer peace of mind. Whether you're at job or on holiday, the smart home will aware you to what's going on, and security system can be built to offer some help in emergency situations. For example, not only would a house owner be woken with warning of a fire alarm, the smart home would also release doors, call the fire department and light the pathway to safety (Saxena et al., 2012).

1.2 STATEMENT OF THE PROBLEM

Traditional door lock systems, while widely used, are often prone to vulnerabilities such as key duplication, lock picking, and limited accessibility. These limitations pose significant security risks and challenges for users seeking convenience and enhanced control over home access.

The advent of Internet of Things (IoT) technology offers an opportunity to transform conventional locking mechanisms into intelligent, automated systems capable of addressing these shortcomings. However, implementing a reliable and user-friendly IoT-based smart door lock system presents challenges, including ensuring robust security, seamless connectivity, and efficient operation. Existing solutions may also lack cost-effectiveness or compatibility with diverse user needs

1.3 AIM AND OBJECTIVES OF THE STUDY

The aim of this study is to design and implement a smart door lock system using IoT technology that enhances home security, improves user convenience, and integrates seamlessly with modern home automation systems. The objectives of the study are:

i. To develop a smart door lock system that utilizes IoT technology for remote access and control.

ii. To ensure robust security features, including real-time authentication and alerts.

iii. To design a user-friendly interface for easy management and monitoring of the lock system.

iv. To integrate the system with existing smart home automation platforms for seamless operation.

v. To evaluate the performance, reliability, and cost-effectiveness of the implemented system.

1.4 METHODOLOGY

This research employs a structured approach to design and implement a smart door lock system using IoT technology. The system's hardware components, including microcontrollers, sensors, and actuators, will be selected and assembled to enable remote access and control. Secure communication protocols, such as MQTT or HTTPS, will be utilized to ensure robust security features, including real-time authentication and alerts. A user-friendly interface will be developed through a mobile or web application, allowing users to manage and monitor the system efficiently. Integration with existing smart home automation platforms will be achieved using APIs or compatible IoT frameworks to ensure seamless operation. The system will undergo rigorous testing to evaluate its performance, reliability, and cost-effectiveness. Both qualitative and quantitative data will be analyzed to assess the system's functionality and user satisfaction, ensuring the objectives are met effectively.

1.5 SCOPE OF THE STUDY

This study focuses on the design and implementation of a smart door lock system using IoT technology for home automation. The research encompasses the development of hardware and software components necessary for remote access, real-time monitoring, and secure authentication. The system will be designed to integrate with existing smart home platforms, allowing seamless operation within a connected home environment. The study targets residential applications, emphasizing affordability, reliability, and ease of use for end users. It will not cover large-scale industrial or commercial security systems but will provide a foundation for scaling IoT-based solutions to similar domains. Testing and evaluation will be conducted under controlled conditions to assess performance, security, and cost-effectiveness. The study is limited to IoT-enabled smart door lock prototypes and does not include long-term deployment or maintenance beyond the scope of the research duration.

1.6 LIMITATION OF THE STUDY

This study is subject to certain limitations that may influence its outcomes. First, the research focuses on a prototype of the smart door lock system, which may not fully replicate real-world deployment scenarios. The system's performance is tested under controlled conditions, limiting its evaluation in diverse environmental or network settings. Second, the reliance on IoT technology means the system is dependent on stable internet connectivity; interruptions could affect functionality. Third, the integration with existing smart home platforms is confined to commonly used frameworks, which may restrict compatibility with less popular systems. Fourth, the study prioritizes cost-effectiveness, which may limit the use of advanced materials or high-end components. Lastly, the research does not address potential long-term maintenance or evolving cybersecurity threats, which may impact the system's durability and security over time. These limitations provide areas for further investigation and improvement in future research.

1.7 OPERATIONAL DEFINITION OF TERMS

1. **Smart Door Lock System**: A technologically advanced locking mechanism that allows users to remotely lock and unlock doors, monitor access, and enhance security through IoT integration.

2. **Internet of Things (IoT)**: A network of interconnected devices that communicate and exchange data over the internet to enable automation and remote control.

3. **Home Automation**: The use of technology to control and automate home devices and systems, such as lighting, security, and appliances, to enhance convenience and efficiency.

4. **Authentication**: The process of verifying the identity of a user or device to ensure authorized access to the smart door lock system.

5. **Real-Time Monitoring**: The capability to track and observe the status or activities of the smart door lock system instantaneously via a connected device.

6. **User-Friendly Interface**: A simple and intuitive design of the system's application or control platform that enables easy management by users.

7. **Integration**: The process of connecting the smart door lock system with other home automation devices or platforms for seamless operation.

8. **Cybersecurity**: Measures and technologies implemented to protect the system from unauthorized access, hacking, or data breaches.

1.8 ORGANIZATIONS OF THE REPORT

This research work is divided into five chapter as follows:

Chapter one discusses the Background to the study, Statement of the problem, Aim and Objectives of the study, Methodology, Scope of the Study, Limitation of the Study, Operational Definition of terms and Organization of the report. All this outlines the detailed objectives to achieve the main goals of this research work. Chapter two focus on past researches (Review of related literature), Overview of Design and Implementation of Smart Door Locked System Using IoT Home Automation. Chapter three evaluate the Description of the Existing System, Problem of the Traditional System, Description of the proposed system, Circuit Diagram and Architectural Design of the proposed system. Chapter four emphasize on Overall Design of the research work Design and Implementation of Smart Door Locked System Using IoT Home Automation.). Chapter will provide a clear structure for this research work, each chapter will focus and contributes to the overall understanding of Design and Development of IOT based smart inverter energy controlling system.

CHAPTER TWO

LITERATURE REVIEW

2.1 REVIEW OF RELATED WORKS

In this section, researches and journals related to this work is broadly highlights.

Shiu Kumar (2015) proposed smart home design application that allows owner to manage their home through internet. Its need a PC tend the information to the internet, so a PC is used as a server that increases the price and power consumption while others need web page hosting that need extra cost also.In his paper, said that the use of PC can require considerable cost and can be reduced by using a microcontroller (Liu and Zhang, 2022). Deepali recommends the use of the android platform version 2.3.4 Gingerbread and 3.1 Honeycomb using the Java programming language for smart home security system for the disabled and senior citizens (John et al., 2013). In his research, the connection between android platform and the home device using wired conection, so It will be more efficient to support various wired as well as wireless technologies such as Bluetooth, Zigbee, Wi-Fi, World Wide Web.

The implementation of Bluetooth for home security systems using the ARM9 processor were introduced by Naresh (2018). Hao Shi, in his research on home lighting settings implemented an open-source Android Development Tools (ADT), the Android SDK (Software Development Kit) and Java Development Kit (JDK) [9]. Manasee Patil had examined home automation system using RFID, Wireless Sensor Network (ZigBee) technology and GSM. ZigBee is low power wireless technology used for monitoring and controlling various devices [10]. R. Piyare [11] has introduced design and implementation of a low cost, flexible and wireless solution for home automation, especially or on/off the lamp and to on/off the television automatically. However, this is a basic system without advanced features like integration of RTOS, and also not has light sensors that are used to intelligently control the home appliances without human intervention.

ECHO IV and the Kitchen Computer developed in the late 1960s were about the first smart devices though they were not commercially sold. The devices could compute shopping lists, control the home temperature and turn appliances on or off and the Kitchen Computer, developed a year later, could also store recipes. In 1991, GERONTECHNOLOGY- a combination of gerontology and technology was developed to make the lives of senior citizens easier and better. Later advances in technology and services grew in bounds, and a telemonitoring system based on a Short Message Service (SMS), to remotely monitor the long-term mobility levels of elderly people in their natural environment were introduced. To measure the mobility of subjects, an accelerometer-based portable unit are worn by each monitored subject.

An Internet-based monitoring and control of fuzzy controlled inverter for air conditioning system was developed by Yen-Shin Lai in 2002. The system consists of client/server, programmable logic controller, D/A modules, inverters, induction motors and the temperature sensing modules. The client accepts the command from the user and can also access the database created in server, using Internet Explorer (IE) Browser. The server performs function of fuzzy logic control, communication interface between server and Programmable Logic Controller(PLC), and receiving command from client. Furthermore, the server also creates a database of the sensed temperature, speed of inverter-controlled motor drives, and reference command A home security system was implemented by Alheraish; 2010, by means of GSM cellular communication network using microcontroller 89X52 and Sony Ericsson GM-47 GSM module. This system enables far end user through SMS facility to monitor the state of home door, provide password facility for key based door lock and control home lighting system. A Java based home automation system via World

Wide Web (WWW) was developed in 2014 by Al-Ali and Al-Rousan. The home appliances were controlled from ports of embedded system board connected to PC based server at home. The system is scalable and allows multivendor appliances to be added with no major changes to its core. Password protection is used to block unauthorized users from accessing the appliances at home. If the Internet connection is down or the server is not up, the embedded system board still can control and operate the appliances locally. (Al-Ali, 2014)

In the case of (Cliodhna, 2006), the portable unit, houses the Analog Devices ADuC812S microcontroller board, Falcon A2D-1 GSM modem, and a battery-based power supply. Two integrated accelerometers are connected to the portable unit through the analog inputs of the microcontroller. Mobility level summaries are transmitted hourly, as an SMS message, directly from the portable unit to a remote server for long-term analysis. Each subject's mobility levels are monitored using custom-designed mobility alert software, and the appropriate medical personnel are alerted by SMS if the subject's mobility levels decrease.

A system for early diagnosis of hypertension and other chronic diseases was proposed by(Jiang, 2008). The proposed design consists of three main parts: a wrist Blood Pressure (BP) measurement unit, a server unit and a terminal unit. Blood Pressure is detected using data acquired by sensors intelligently using DSP microchip. The data is then transmitted to the remote server unit located at Community Healthcare Centers/Points (CHC/P) by using Short Messaging Service (SMS), and notification information is sent to the terminal unit to inform users if patient's BP is abnormal). Chen Peijiang and Jiang Xuehua, in 2008, came up with a system in which they described a remote monitoring system based on SMS of GSM. The system includes two parts: the monitoring centre and the remote monitoring station. A home automation system based on Wireless Sensor Networks (WSNs) and General Packet Radio Service (GPRS) was proposed by (Jianshe, 2012) that allowed its users to control equipment in their home, and collect data about a device’s status and weather conditions at home through their mobile devices. The authors’ custom-made the application for China, as users receive information about home intrusions and fire through the Chinese Instant Message Mobile Service. Unlike other GPRS-based home automations, the proposed system uses an embedded system-based central controller. Current trends in home automation include remote mobile control, automated lights, automated thermostat adjustment, scheduling appliances, mobile/email/text notifications, and remote video surveillance (Hendricks, 2014). A home gateway system for interconnecting home network consisting of IEEE 1394 AV network and X10 power line home automation network with Internet was proposed by Saito in 2009. This provided remote access functions from Internet for digital Audio Visual(AV) appliances like Digital Video Camera, Digital VCR connected to IEEE 1394 network and home appliances like TV, desk lamp, electric fan connected to X10 controller. (Mayur et al., 2015) An iOS-based home automation security system using General Packet Radio Service (GPRS) was developed by S.R. Das. The proposed system uses the client/server model for communication. The authors develop an iOS application that runs on a user’s mobile phone and acts as the client, and the cloud to which the home devices are connected acts as the server. The authors use video cameras, microphones, and motion sensors for providing security at home. When a motion sensor is triggered, the video cameras in the vicinity start to record. A user can view these live feeds on a mobile device through GPRS. The proposed system can also be accessed using a web browser, (Arun, 2017).

Despite these success recorded in home automation systems, John J. Greichen (1992) discussed challenges faced to include high manufacturing costs, high development costs, high installation costs, additional service and support costs, lack of home automation standards, consumer unfamiliarity with technology, and complex user interfaces. Today’s Smart Homes are more about security, alerting us about unauthorized intrusion, living greener, sustainability, and they help to ensure that our homes reduce unnecessary energy waste.

2.2 REVIEW OF RELATED CONCEPTS

2.2.1 Overview of Smart Door Lock System

Smart door lock systems represent a transformative advancement in the realm of home security, offering enhanced convenience, flexibility, and control. These systems leverage the capabilities of modern technologies, such as the Internet of Things (IoT), to overcome the limitations of traditional locks and meet the growing demand for intelligent home automation solutions.

At their core, smart door locks incorporate electronic components like microcontrollers, sensors, and communication modules. These components enable users to remotely control access to their doors, monitor real-time activity, and receive alerts via connected devices. Unlike traditional locks, which rely solely on mechanical keys, smart locks often utilize alternative access methods such as PIN codes, biometric authentication (e.g., fingerprint or facial recognition), or mobile applications. This diversity in authentication methods enhances security while offering greater flexibility for users (Smith & Brown, 2020).

IoT technology serves as the backbone of smart door lock systems, providing seamless connectivity and data exchange between devices. Through IoT, smart locks can communicate with cloud services and mobile applications, enabling remote control and monitoring. This functionality is particularly beneficial in scenarios such as granting temporary access to guests or service providers without the need for physical keys (Johnson et al., 2021). Furthermore, IoT integration facilitates the automation of smart locks within a broader home automation ecosystem, allowing for centralized control alongside other devices like lighting, thermostats, and surveillance cameras.

The security features of smart door locks are a key area of innovation. Many systems employ end-to-end encryption and secure communication protocols, such as HTTPS or MQTT, to safeguard against cyber threats. Additionally, smart locks often provide real-time alerts for unauthorized access attempts, offering an extra layer of security. For instance, systems equipped with tamper detection mechanisms can notify users immediately if someone attempts to manipulate the lock physically (Lee & Kim, 2019).

User experience is another critical factor in the design of smart door lock systems. A well-designed user interface, typically accessible through a mobile or web application, ensures ease of operation. Features such as one-touch locking/unlocking, access logs, and integration with voice assistants like Amazon Alexa or Google Assistant significantly enhance usability. These interfaces are designed to accommodate users of all technical proficiency levels, making smart locks accessible to a broader audience (Garcia et al., 2022).

Despite their numerous advantages, smart door lock systems face certain challenges. Dependence on stable internet connectivity is a notable limitation, as disruptions can hinder the lock's functionality. Additionally, the cost of smart locks may be a barrier for some users, particularly when compared to traditional locks. However, ongoing advancements in IoT technology and increasing competition in the market are expected to drive down costs and improve reliability over time (Williams, 2021).

Smart door lock systems epitomize the potential of IoT technology in enhancing home security and automation. By combining advanced security features, user-friendly interfaces, and seamless integration with other smart devices, these systems address the evolving needs of modern homeowners. As technological innovations continue to address existing challenges, smart door locks are poised to become an integral component of the connected home ecosystem.

2.2.2 Overview of Internet of Things (IoT)

The Internet of Things (IoT) is a revolutionary technological concept that refers to a network of interconnected devices capable of communicating and exchanging data over the internet without requiring direct human intervention. IoT has transformed industries by enabling the integration of physical objects with digital systems, leading to enhanced automation, efficiency, and connectivity (Ashton, 2009).

IoT operates through a combination of sensors, actuators, communication technologies, and data analytics. Devices embedded with sensors collect data from their environment, which is then transmitted through communication protocols like Wi-Fi, Bluetooth, or Zigbee to a central hub or cloud platform. This data is processed and analyzed to trigger automated responses or provide actionable insights. The integration of IoT across various sectors has led to significant advancements in areas such as healthcare, agriculture, transportation, and home automation (Atzori et al., 2010).

One of the most prominent applications of IoT is in smart home automation. IoT-enabled devices, such as smart thermostats, lighting systems, and door locks, allow homeowners to monitor and control their environments remotely. These systems provide convenience, energy efficiency, and enhanced security by leveraging real-time data and automation capabilities (Vermesan & Friess, 2014). For instance, a smart thermostat can learn user preferences and automatically adjust the temperature, optimizing energy consumption. Similarly, IoT-based door locks offer remote access and monitoring features, addressing modern security needs (Lee & Kim, 2017).

IoT is also playing a transformative role in healthcare through applications like remote patient monitoring, wearable devices, and telemedicine. These technologies enable real-time tracking of health metrics, early detection of medical conditions, and improved access to care, particularly in remote areas. In agriculture, IoT facilitates precision farming, where sensors monitor soil moisture, weather conditions, and crop health, optimizing resource utilization and improving yields (Patel & Patel, 2016).

Despite its potential, IoT faces several challenges, particularly in the areas of security and privacy. As devices collect and transmit sensitive data, they become attractive targets for cyberattacks. Ensuring robust encryption, secure communication protocols, and regular software updates are essential to mitigating these risks (Roman et al., 2011). Additionally, the interoperability of IoT devices across different manufacturers and platforms remains a significant hurdle. Standardization efforts are underway to address these issues, promoting seamless integration and collaboration across IoT ecosystems (Perera et al., 2014).

The rapid growth of IoT is fueled by advancements in enabling technologies such as 5G, artificial intelligence (AI), and edge computing. These innovations are enhancing the scalability, speed, and intelligence of IoT systems, paving the way for more sophisticated applications. For example, 5G networks provide the low latency and high bandwidth needed for real-time IoT applications, while AI enables predictive analytics and decision-making (Friess, 2016).

In conclusion, IoT is a transformative force that is reshaping industries and improving quality of life through its wide-ranging applications. While challenges related to security, privacy, and interoperability persist, ongoing technological advancements and standardization efforts are driving IoT toward becoming an integral part of the global digital landscape.

2.2.3 Overview on Authentication and Security

Authentication and security are critical components of modern digital systems, especially in the era of interconnected devices and services. Authentication involves verifying the identity of users, devices, or systems to ensure access is granted only to authorized entities. Security encompasses the measures and practices designed to protect systems, data, and communications from unauthorized access, cyber threats, and potential breaches. Together, these elements form the foundation of trust and reliability in digital ecosystems (Kumar et al., 2018).

Authentication mechanisms have evolved significantly over the years, moving beyond simple passwords to include more robust methods. Password-based authentication, while still prevalent, is increasingly vulnerable to attacks like phishing and brute force. To address these challenges, multi-factor authentication (MFA) has gained prominence, requiring users to provide two or more forms of verification, such as something they know (password), something they have (security token), or something they are (biometric data). Biometric authentication, which includes fingerprints, facial recognition, and retina scans, is particularly valued for its convenience and difficulty to replicate (Jain et al., 2016).

In IoT systems, authentication plays a crucial role in ensuring that devices and users can trust each other. Lightweight authentication protocols are often employed in resource-constrained devices to minimize computational overhead while maintaining security. Examples include elliptic curve cryptography (ECC) and message authentication codes (MAC) (Al-Fuqaha et al., 2015). Furthermore, device-to-device authentication is essential to prevent unauthorized devices from joining the network or accessing sensitive information.

Security measures in digital systems aim to protect data integrity, confidentiality, and availability. Cryptographic techniques such as encryption are commonly used to secure data during transmission and storage. Protocols like Transport Layer Security (TLS) and Secure/Multipurpose Internet Mail Extensions (S/MIME) ensure secure communication over public networks. End-to-end encryption, a practice where data is encrypted at the sender's end and decrypted only at the receiver's end, is increasingly adopted in applications ranging from messaging platforms to IoT systems (Dierks & Rescorla, 2008).

Despite advancements, several challenges persist in the domains of authentication and security. The rise of sophisticated cyberattacks, such as man-in-the-middle (MITM) attacks, ransomware, and distributed denial-of-service (DDoS) attacks, has underscored the need for continuous innovation. IoT devices, in particular, are vulnerable due to their limited computational power and often insufficient security measures. Solutions such as blockchain for secure and decentralized authentication, as well as AI-driven anomaly detection, are being explored to address these vulnerabilities (Raman et al., 2020).

Regulatory frameworks also play a vital role in strengthening authentication and security. Standards such as the General Data Protection Regulation (GDPR) in the European Union and the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) in the United States guide organizations in implementing best practices. Compliance with these standards helps build user trust and ensures accountability in the event of breaches (Arora et al., 2019).

In conclusion, authentication and security are indispensable in safeguarding digital interactions. As technology continues to evolve, the integration of advanced mechanisms and adherence to robust frameworks will be essential in addressing emerging threats and ensuring the integrity of systems and data.

2.2.4 Overview on Home Automation Integration

Home automation integration refers to the seamless connection and coordination of various smart devices and systems within a household, enabling centralized control, improved convenience, and enhanced efficiency. By leveraging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, home automation systems allow users to manage lighting, heating, security, and entertainment systems through centralized platforms, often controlled via smartphones, voice assistants, or dedicated control panels (Balta-Ozkan et al., 2014).

At the core of home automation integration is IoT technology, which facilitates communication among devices through wireless protocols like Wi-Fi, Zigbee, Z-Wave, and Bluetooth. These protocols enable interconnected devices to exchange data and respond to user commands or predefined triggers. For instance, a smart thermostat can adjust the temperature based on occupancy sensors, while smart lighting systems can automatically dim or turn off lights when rooms are unoccupied (Perera et al., 2014).

A key aspect of successful integration is interoperability, which ensures that devices from different manufacturers can work together seamlessly. Many home automation platforms, such as Amazon Alexa, Google Home, and Apple HomeKit, provide unified ecosystems that support a wide range of devices. These platforms enable centralized control, allowing users to manage their entire smart home setup through a single interface or voice commands. For example, users can create routines such as "Good Night," which turns off lights, locks doors, and adjusts the thermostat with one command (Yang et al., 2017).

Security and privacy are critical considerations in home automation integration. With multiple devices connected to the internet, ensuring data security and protecting user privacy are paramount.

Encryption protocols, secure authentication methods, and regular firmware updates are essential to mitigate risks such as unauthorized access, data breaches, and cyberattacks. Additionally, advanced platforms now include features like encrypted local control, which reduces dependence on cloud services for executing commands, enhancing security and reliability (Sicari et al., 2015).

Energy efficiency is another significant benefit of home automation integration. Smart systems optimize energy consumption by automating tasks like adjusting HVAC systems based on room usage or scheduling appliances to run during off-peak hours. Studies have shown that integrated home automation systems can lead to substantial energy savings and reduced utility costs, aligning with global sustainability goals (Marikyan et al., 2019).

Despite its advantages, home automation integration faces challenges, including the high cost of initial setup, compatibility issues among devices, and the need for robust internet connectivity. Standardization efforts, such as the Matter protocol, are being developed to address these challenges by establishing universal communication standards for smart home devices. As these protocols gain adoption, the barriers to entry for consumers are expected to decrease, making home automation more accessible to a wider audience (Zou et al., 2020).

Home automation integration represents a significant leap forward in enhancing the quality of life through convenience, security, and efficiency. As technologies continue to evolve and standardization improves, integrated smart homes are likely to become an essential part of modern living, offering a highly connected and optimized domestic environment.

2.2.5 Overview on Performance Evaluation Smart Door System using IoT Home Automation

Performance evaluation is a systematic process of assessing the efficiency, effectiveness, and reliability of a system, product, or process. In technology and engineering, it plays a critical role in determining whether a system meets predefined goals, operates optimally under various conditions, and satisfies user requirements. Performance evaluation provides actionable insights for improvement, ensuring the delivery of high-quality outcomes (Jain, 1991).

A well-conducted performance evaluation typically involves setting measurable objectives, selecting evaluation criteria, and employing appropriate methodologies. Metrics such as speed, accuracy, reliability, scalability, and cost-effectiveness are commonly used to assess performance. These metrics vary based on the system being evaluated. For example, in computing, response time, throughput, and resource utilization are key indicators, while in IoT systems, latency, energy efficiency, and device interoperability are emphasized (Kansal et al., 2010).

Performance evaluation methodologies are generally categorized into three approaches: analytical modeling, simulation, and experimental testing. Analytical models use mathematical frameworks to predict system behavior under different scenarios. Simulation involves creating virtual representations of a system to test its performance in controlled environments, often utilizing software tools such as MATLAB or NS2. Experimental testing, on the other hand, involves deploying the system in real-world conditions to collect empirical data. Each method has its strengths and limitations; analytical modeling offers speed and cost-effectiveness, while experimental testing provides highly accurate results (Banks et al., 2010).

In IoT systems, performance evaluation is particularly crucial due to their complexity and the diversity of use cases. For instance, an IoT-based smart door lock system may be evaluated based on parameters such as authentication speed, energy consumption, and resistance to cyberattacks. Ensuring low latency in remote access, consistent operation under varying network conditions, and robust security features are essential for achieving user satisfaction and reliability (Al-Fuqaha et al., 2015).

Challenges in performance evaluation often arise from the dynamic and unpredictable nature of real-world environments. Systems may behave differently under varying conditions, such as high user loads or network interruptions. Additionally, emerging technologies like machine learning and IoT present unique challenges due to their reliance on large-scale data processing and real-time decision-making. These complexities necessitate the development of advanced evaluation tools and frameworks to provide comprehensive insights (Zhou et al., 2018).

Another key aspect of performance evaluation is benchmarking, which involves comparing a system's performance against industry standards or competitors. Benchmarking helps identify strengths, weaknesses, and areas for improvement. For instance, in the context of smart home automation, benchmarking a smart door lock system against other market solutions can highlight competitive advantages, such as faster authentication times or better energy efficiency (Kumar et al., 2016).

In conclusion, performance evaluation is a cornerstone of system development and optimization, ensuring that systems meet user expectations and operate effectively in diverse conditions. By employing rigorous methodologies, leveraging advanced tools, and addressing emerging challenges, performance evaluation continues to drive innovation and reliability across various domains.

CHAPTER THREE

RESEARCH METHODOLOGY

2.1 DESCRIPTION OF THE EXISTING SYSTEM

The existing systems for door lock management primarily rely on traditional mechanical locks or electronic locks with limited functionality. Mechanical locks, while simple and cost-effective, depend solely on physical keys, making them prone to issues like key loss, duplication, and tampering. These locks provide minimal security features and do not allow remote access or real-time monitoring.

Electronic locks, including keypad-based systems and card access systems, offer some level of advancement over mechanical locks. Users can unlock doors by entering a PIN or using RFID-enabled cards. These systems eliminate the need for physical keys but come with their own limitations. For instance, PIN-based locks are susceptible to shoulder surfing, and RFID cards can be cloned if not adequately secured. Moreover, these systems lack advanced features like remote access, user authentication logs, and integration with smart home systems.

In recent years, some smart door lock systems have entered the market, incorporating basic Internet of Things (IoT) features. These systems often provide functionalities such as unlocking via smartphone apps, temporary access codes, and activity notifications. However, many of these existing solutions have significant drawbacks, including limited interoperability with other smart devices, high power consumption, and vulnerabilities to cyberattacks due to weak encryption protocols. Additionally, they often require proprietary platforms, creating compatibility challenges for users who wish to integrate them into broader smart home ecosystems.

Lastly, the existing systems, while offering incremental improvements, fail to address the growing demand for robust security, ease of use, and seamless integration. They lack the advanced features and comprehensive design needed to meet the evolving needs of modern users, particularly in the context of smart home automation and IoT advancements.

3.2 PROBLEMS OF THE EXISTING SYSTEM

1. **Reliance on Physical Keys**: Traditional mechanical locks depend entirely on physical keys, which can be easily lost, stolen, or duplicated. This reliance creates vulnerabilities in security and convenience, especially in situations requiring frequent access management.

2. **Limited Access Control**: Mechanical locks and basic electronic locks do not offer fine-grained access control. Users cannot set time-based access permissions or provide temporary access remotely, making these systems unsuitable for modern, dynamic access requirements.

3. **Susceptibility to Tampering**: Mechanical locks are prone to physical tampering, such as lock picking or bumping. Similarly, basic electronic locks are vulnerable to power disruptions and lack mechanisms to prevent unauthorized entry through technical exploits.

4. **Lack of Remote Access**: Most existing systems do not support remote access or monitoring. Users cannot lock or unlock doors from distant locations, view real-time access logs, or receive notifications about attempted breaches, limiting their usability in connected environments.

5. **Compatibility Challenges**: Many smart locks in the current market are designed to operate within proprietary ecosystems, making it difficult for users to integrate them with other

smart home devices or platforms. This lack of interoperability hinders seamless automation.

6. **Cybersecurity Vulnerabilities**: Basic smart locks often suffer from weak encryption protocols or lack proper firmware updates, exposing them to cyberattacks such as hacking or unauthorized access through compromised devices.
7. **High Power Consumption**: Existing IoT-enabled locks frequently exhibit poor power management, leading to short battery life. This results in increased maintenance needs and potential lockouts when the power supply is depleted.
8. **User Interface Limitations**: Many electronic and smart locks have unintuitive interfaces, making them difficult to configure or use, especially for non-technical users. This reduces user satisfaction and adoption rates.

These problems highlight the need for a more robust, secure, and user-friendly smart door lock system that leverages IoT technology for advanced functionality and seamless integration.

3.3 DESCRIPTION OF THE PROPOSED SYSTEM

The proposed system is a smart door lock solution that leverages Internet of Things (IoT) technology to enhance security, usability, and integration with modern home automation platforms. Unlike traditional mechanical or basic electronic locks, the system offers advanced features such as remote access, real-time monitoring, and seamless connectivity, addressing the limitations of existing systems.

The smart door lock will be equipped with multiple authentication methods, including biometric scanning (e.g., fingerprint recognition), mobile app control, and PIN entry. These features ensure robust security by providing multi-factor authentication while also catering to diverse user preferences. Remote access will enable users to lock or unlock doors, monitor activity logs, and manage access permissions from anywhere through a secure smartphone application.

To enhance security, the system will include features such as real-time alerts for unauthorized access attempts, encryption protocols to secure data transmission, and regular firmware updates to address emerging threats. Integration with existing smart home ecosystems, such as Amazon Alexa, Google Home, or Apple HomeKit, will allow users to incorporate the lock into broader automation routines, such as locking doors automatically when leaving home or integrating with security cameras for a comprehensive solution.

The system will also prioritize energy efficiency by utilizing low-power components and notifying users when battery levels are low, reducing the risk of unexpected lockouts. The user interface will be designed for ease of use, with a straightforward setup process and intuitive controls.

By addressing the limitations of existing systems and incorporating advanced IoT capabilities, the proposed smart door lock system will provide a secure, user-friendly, and scalable solution tailored to modern home automation needs.

3.3.1 Advantages of the Proposed System

The proposed system delivers a comprehensive, secure, and convenient solution tailored to modern lifestyles and smart home environments. Below are some of advantages

1. **Enhanced Security**: The proposed system incorporates advanced authentication methods such as biometrics, PINs, and mobile app control, ensuring robust security and minimizing vulnerabilities associated with traditional locks. Multi-factor authentication adds an additional layer of protection against unauthorized access.

2. **Remote Access and Control**: Users can lock or unlock doors from any location using a secure smartphone app. This feature is particularly useful for granting temporary access to visitors, monitoring real-time activity logs, or locking doors remotely for added peace of mind.

3. **Real-Time Notifications**: The system provides instant alerts for suspicious activities, such as unauthorized access attempts or tampering. This ensures users are always aware of their door lock's status and can take immediate action if needed.

4. **Integration with Smart Home Ecosystems**: Seamless compatibility with platforms like Amazon Alexa, Google Home, and Apple HomeKit allows the smart lock to work in harmony with other smart devices. Users can incorporate the lock into automation routines for added convenience, such as locking doors automatically when leaving or integrating with security cameras for enhanced surveillance.

5. **Energy Efficiency**: The system is designed to consume minimal power, extending battery life and reducing maintenance requirements. Low-battery alerts further enhance usability by notifying users to replace batteries before they are completely drained.

6. **Ease of Use**: A user-friendly interface ensures simple setup and operation, catering to both tech-savvy and non-technical users. The intuitive design eliminates the complexity often associated with smart devices.

7. **Scalability and Flexibility**: The system supports multiple users, with customizable access levels and schedules. This makes it ideal for households, offices, or rental properties where access needs vary among users.

8. **Improved Safety**: With features like automated locking, tamper detection, and integration with home security systems, the smart lock enhances overall safety and reduces the likelihood of breaches.

3.4 PROPOSED SYSTEM ARCHITECTURE

The proposed smart door lock system architecture is designed to offer secure, efficient, and seamless operation by integrating IoT technology with various components. The architecture consists of several key layers, each serving a specific purpose to ensure the functionality, security, and user-friendliness of the system.

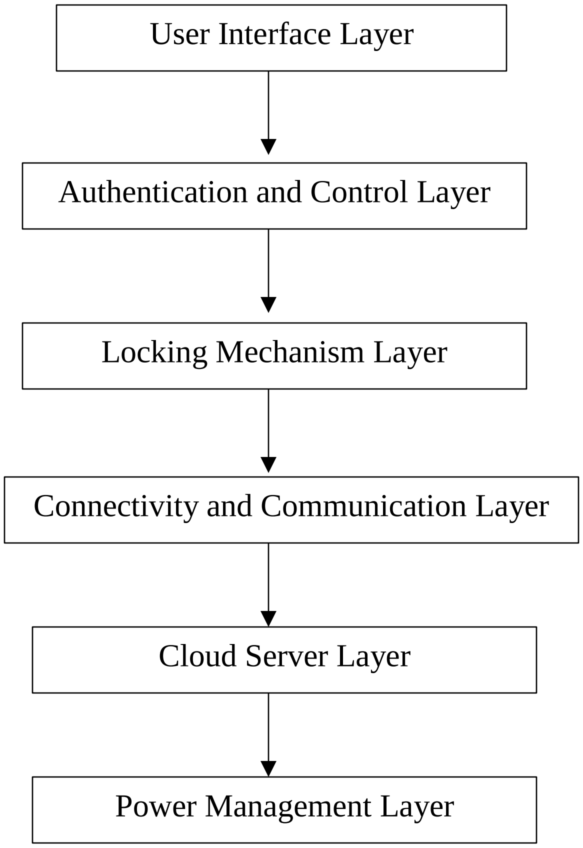


Fig: 3.4: Proposed System Architecture Diagram

Together, these layers form a cohesive system that ensures secure, reliable, and user-friendly operation, providing a modern solution for smart door locking in a connected home environment.

3.5 CIRCUIT DIAGRAM OF THE PROPOSED SYSTEM

The circuit diagram for the proposed "Design and Implementation of Smart Door Lock System Using IoT Home Automation" involves several key components:

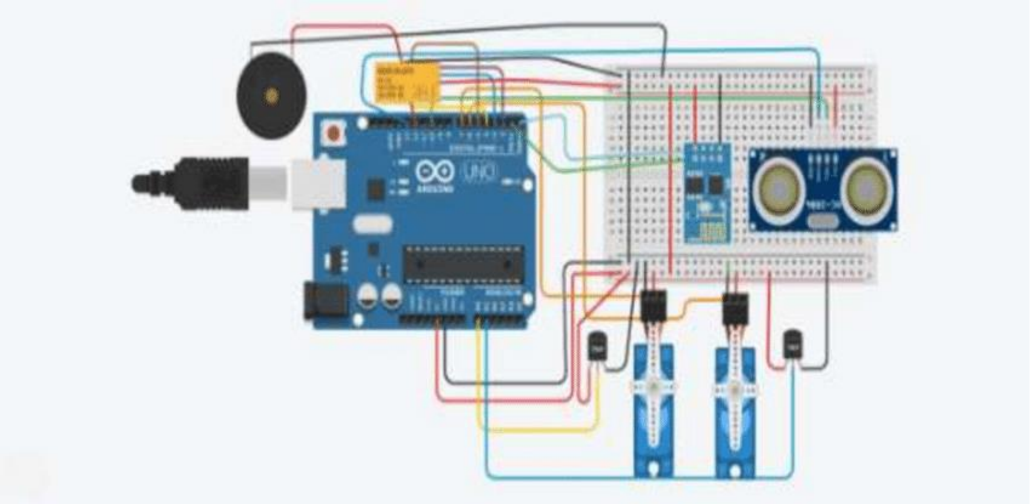


Fig: 3.5: Proposed Circuit Diagram

1. Microcontroller: The central component is a microcontroller such as an Arduino or ESP32. It handles all operations, including receiving input from sensors and controlling output to the lock.

2. RFID Module: The RFID reader is used for authentication. It reads RFID tags and sends the data to the microcontroller for verification. If the tag matches the database, the system activates the door lock mechanism.

3. Servo Motor: The servo motor is used to lock and unlock the door. The servo is controlled by the microcontroller based on authentication results from the RFID reader.

4. Wi-Fi Module: A Wi-Fi module like ESP8266 or ESP32 connects the system to the home automation network, enabling remote control via a smartphone app.

5. Buzzer and LEDs: A buzzer is used to give feedback to the user, indicating success or failure of the authentication process. LEDs (Green/Red) are used to signal lock status—green for unlocked and red for locked.

6. Power Supply: A regulated power supply is used to power the entire system. It typically consists of a DC power source (5V or 12V) to support the microcontroller, sensors, and actuators.

7. Relay: The relay module is connected to the microcontroller and controls the power to the locking mechanism. When the authentication is successful, the relay triggers the lock mechanism.

In this system, the microcontroller coordinates the interaction between all components. The user can either scan an RFID card for entry or remotely control the lock via the IoT app, while the feedback is provided through LEDs and a buzzer. The circuit is designed to be low power and efficient for continuous operation in a home automation environment.

CHAPTER FOUR

DESIGN, IMPLEMENTATION AND DOCUMENTATION OF THE SYSTEM

4.1 SCHEMATICS DESIGN

The schematic design of the smart door lock system using IoT technology outlines the interconnection of hardware components to achieve secure, remote-controlled access to a physical door. At the heart of the design is an ESP32 microcontroller, chosen for its integrated Wi-Fi and Bluetooth capabilities, enabling seamless communication with mobile devices and cloud platforms. The system incorporates a biometric fingerprint sensor and a keypad, both interfaced with the microcontroller to allow multiple authentication options. A relay module is connected to control the actuation of a solenoid lock, which physically locks or unlocks the door based on verified input. Power is supplied through a regulated adapter and supported by a rechargeable battery to ensure uninterrupted operation during power outages. The microcontroller communicates with a mobile application via Wi-Fi, allowing users to monitor access history and remotely control the door lock. Security is reinforced by implementing encrypted data transmission between the system and mobile devices. LED indicators provide visual feedback for lock status and authentication success or failure. The schematic ensures modularity, making it easy to maintain and scale, while emphasizing real-time authentication, reliable connectivity, and power efficiency. This design offers a comprehensive and practical solution for modern smart home security needs.

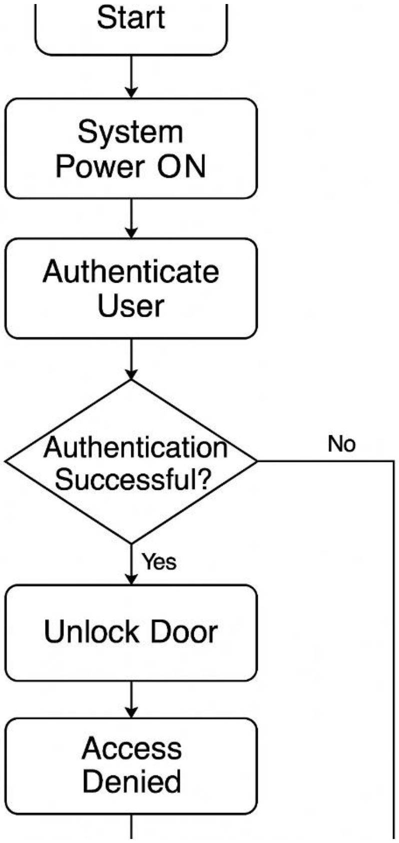
4.2 SYSTEM DESIGN

The system design of the smart door lock using IoT technology is structured to ensure secure access, user convenience, and seamless integration with smart home environments. It consists of both hardware and software components working in unison to provide a reliable locking mechanism. At the core of the system is an ESP32 microcontroller that manages communication, control logic, and device interfacing. Users interact with the system via a mobile application or web interface, which communicates with the microcontroller through Wi-Fi for real-time commands and feedback. Authentication is achieved using a fingerprint sensor and a keypad, allowing for biometric or PIN-based access. The microcontroller processes input data and triggers a relay module to activate a solenoid lock, either locking or unlocking the door accordingly. Notifications and status updates are sent to the user through the mobile app. Additionally, sensors monitor the door’s status, while an onboard LED provides visual indications. The system also includes a power management module with a battery backup to maintain functionality during power outages. The software architecture handles user access control, device management, and logging of entry events. This holistic design ensures flexibility, security, and real-time control, making the system suitable for modern smart homes and office environments.

4.3 SYSTEM DOCUMENTATION

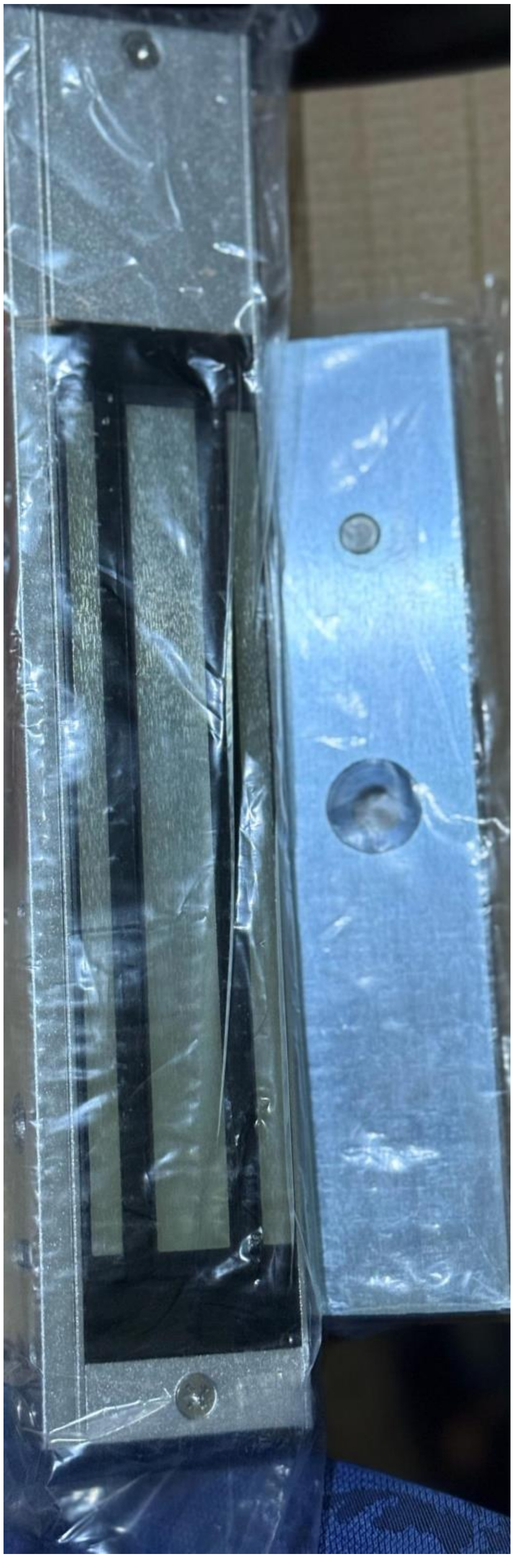
The system documentation for the smart door lock system using IoT provides a comprehensive overview of the development, operation, and management of the project. It includes detailed records of hardware components, software interfaces, and communication protocols used in the implementation. The documentation begins with an explanation of the system architecture, highlighting the integration of the ESP32 microcontroller with key components such as the fingerprint sensor, keypad, relay module, solenoid lock, and power supply. It describes how the system processes user inputs from either biometric or PIN entry and triggers appropriate actions based on authentication results. The documentation also outlines the mobile application functionality, detailing how users remotely monitor and control the door lock via Wi-Fi connectivity. It explains how user credentials and access logs are managed securely, with encryption protocols in place to protect data transmission. Installation guidelines, wiring schematics, and configuration steps are provided to assist with system setup and maintenance. Additionally, it covers troubleshooting procedures, update mechanisms, and scalability considerations. The documentation ensures that users and developers can understand the system's inner workings, replicate or expand it, and maintain it efficiently. It serves as a critical reference for future upgrades and technical support, ensuring the system remains reliable and adaptable.

4.3.1 SYSTEM FLOWCHART



4.4. SYSTEM IMPLEMENTATION

The system implementation of the smart door lock system using IoT technology involves the practical realization of both hardware and software components to deliver a functional and secure locking mechanism. The hardware setup begins with assembling the ESP32 microcontroller, fingerprint sensor, keypad, solenoid lock, and relay module. These components are connected according to the circuit diagram, ensuring each part communicates effectively with the control unit. The microcontroller is programmed using the Arduino IDE, where firmware is uploaded to handle user authentication, sensor inputs, and actuation commands. The system is powered by a regulated adapter with an integrated rechargeable battery for backup. The software implementation includes developing a mobile application interface for users to register, log in, receive notifications, and remotely unlock or lock the door. The app communicates with the microcontroller over Wi-Fi using HTTP or MQTT protocols. Authentication logs are recorded, and real-time alerts are enabled for unauthorized access attempts. Security measures such as encrypted data transfer and user access control are embedded within the system. After installation, the system undergoes functional testing to verify accuracy, reliability, and response time. The successful integration of these components demonstrates the feasibility of a cost-effective, efficient, and scalable smart door locking solution for smart home environments.



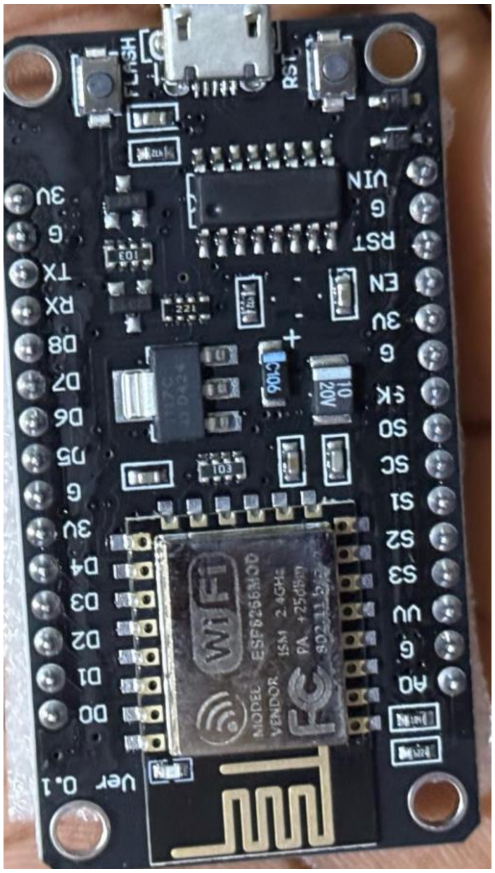


Fig. 4.3: Nod MCU

Fig. 4.2: Magnetic Lock

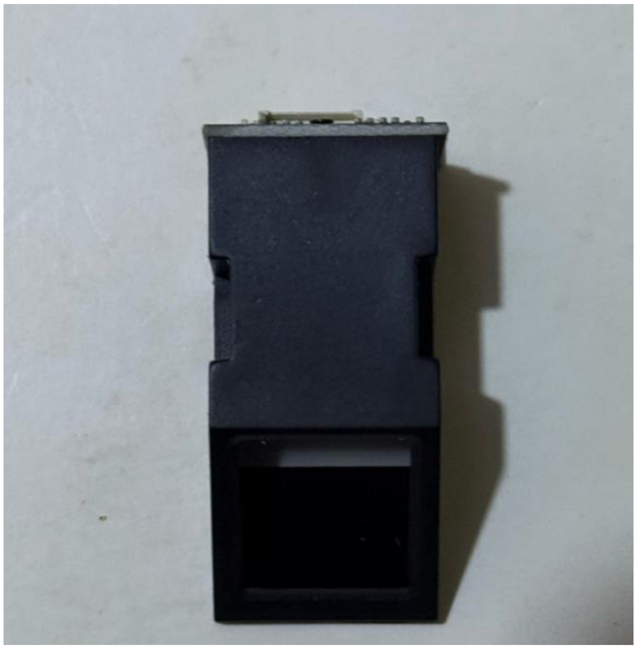


Fig. 4.4: Fingerprint

Fig. 4.5: T& R Cable

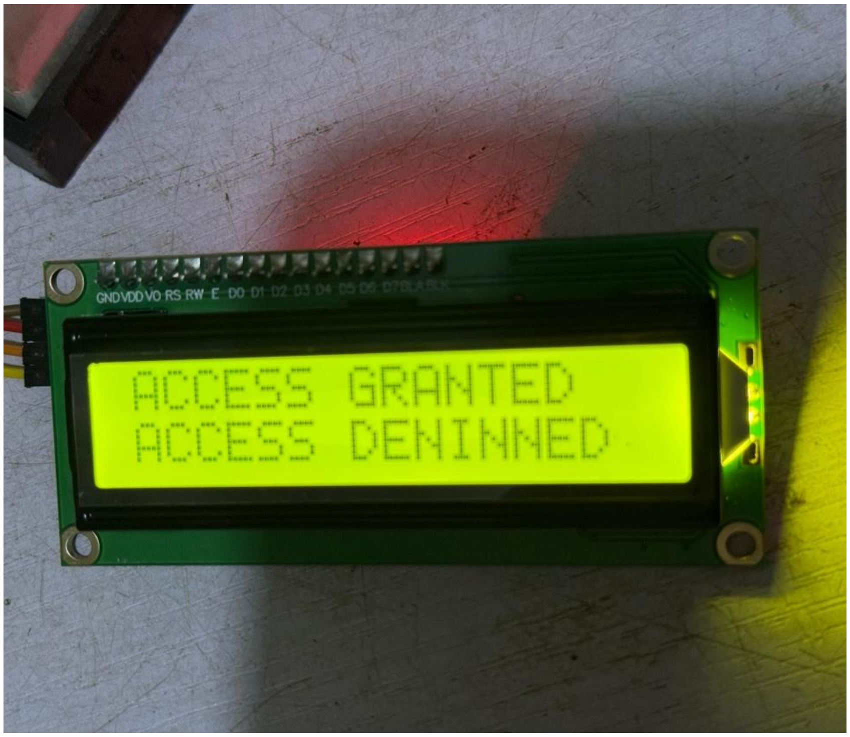


Fig 4.6: LCD

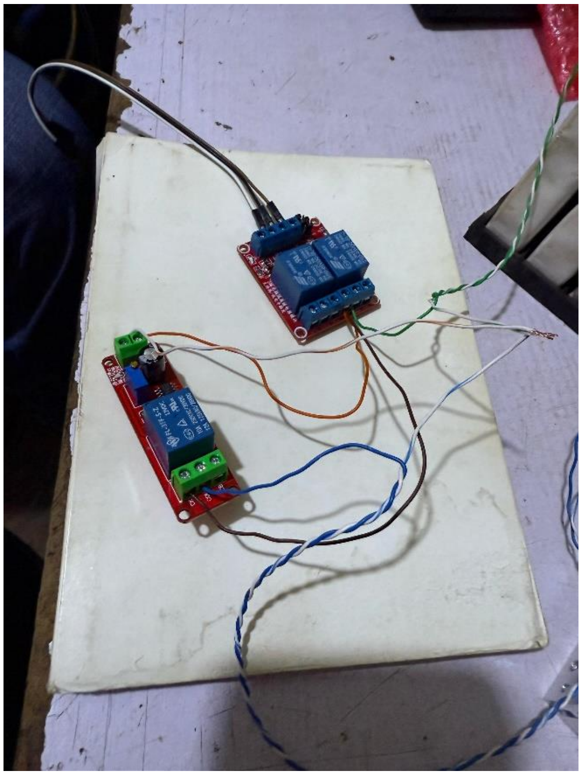


Fig. 4.7 Relay

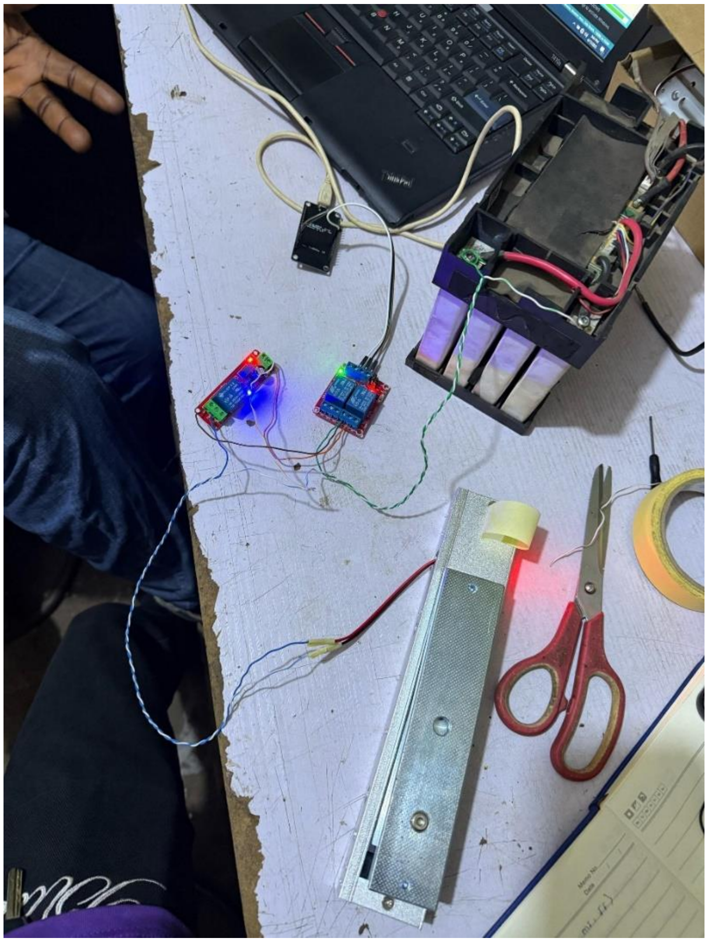


Fig.: 4.8 Battery

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION0053

5.1 SUMARRY

This research focused on the design and implementation of a smart door lock system using IoT home automation to enhance residential and office security. The system integrates modern technologies such as biometric authentication, keypad entry, and wireless communication to provide secure, flexible, and user-friendly access control. Utilizing an ESP32 microcontroller, the system connects with a fingerprint scanner, keypad, relay-controlled solenoid lock, and a mobile application to allow both local and remote operations. Users can lock or unlock the door via fingerprint verification, PIN code, or through the mobile app, offering multiple access options. The system ensures real-time alerts, logs access attempts, and remains functional during power outages through a backup battery. The mobile app, supported by Wi-Fi connectivity, enables remote monitoring and management of the locking system. The implementation process included hardware setup, software development, and system testing to verify performance, security, and reliability. This project demonstrates a cost-effective solution for enhancing home security with IoT technologies. It addresses major limitations of traditional locks, such as key misplacement and lack of remote control. Overall, the research presents a scalable, reliable, and secure smart locking system suitable for integration with other smart home platforms, contributing to the growing field of home automation.

5.2 CONCLUSION

This research focused on the design and implementation of a smart door lock system using IoT home automation to enhance residential and office security. The system integrates modern technologies such as biometric authentication, keypad entry, and wireless communication to provide secure, flexible, and user-friendly access control. Utilizing an ESP32 microcontroller, the system connects with a fingerprint scanner, keypad, relay-controlled solenoid lock, and a mobile application to allow both local and remote operations. Users can lock or unlock the door via fingerprint verification, PIN code, or through the mobile app, offering multiple access options. The system ensures real-time alerts, logs access attempts, and remains functional during power outages through a backup battery. The mobile app, supported by Wi-Fi connectivity, enables remote monitoring and management of the locking system. The implementation process included hardware setup, software development, and system testing to verify performance, security, and reliability. This project demonstrates a cost-effective solution for enhancing home security with IoT technologies. It addresses major limitations of traditional locks, such as key misplacement and lack of remote control. Overall, the research presents a scalable, reliable, and secure smart locking system suitable for integration with other smart home platforms, contributing to the growing field of home automation.

5.3 RECOMMENDATIONS

Based on the findings and successful implementation of the smart door lock system using IoT technology, several recommendations are suggested to enhance the system’s effectiveness and promote future development.

i. First, the integration of cloud-based data storage and analytics is recommended to ensure efficient data logging, backup, and advanced user activity tracking. This would help in maintaining access records and identifying patterns for improved security.

ii. Future versions of the system should consider the inclusion of voice recognition or facial recognition technologies to expand the range of authentication options. This will provide additional convenience and reinforce access control. It is also recommended to adopt more robust encryption protocols to further secure data transmission and prevent potential cyberattacks.

iii. Additionally, the system should be tested under various environmental conditions to ensure consistent performance in different climates and usage scenarios. Expanding compatibility with popular smart home ecosystems like Google Home or Amazon Alexa would enhance user experience and system flexibility.

iv. Lastly, a user education program should be implemented to help users understand the system's features, manage credentials effectively, and maintain security hygiene. By adopting these recommendations, the smart door lock system can be further improved and better positioned for large-scale adoption in modern smart homes.

REFERENCES

Aadel, I.A & Ali, E.T (2020). *Home security system using internet of things* (IOP Conf. Ser. Mater. Sci. Eng) vol, 263 no 4 2017.

Adriansyah & Dani, (2021). *SAFE HOME©* an Advanced Home Security System. 2: 234-239.

Ajao, K.O., Jain, S Bose and L Boppana (2021). *IoT based smart security and home automation system (*Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA) no October 2017 pp 1286–1289

Anitha, A (2021), Design and Implementation of Security Systems for Smart Home based on GSM technology. *International Journal of Smart Home*. 7(6): 201-208.

Bangali & Shaligram, A. (2013). *Design and implementation of security systems for smart home based on GSM technology* (Int. J. Smart Home) vol 7 no 6 pp 201–208

Bimenyimana L. Bhavani Annapurna, K. Mounika, K, Chakradhara Chary, Roohi Afroz (2018). Smart Security System using Arduino and Wireless Communication. *International Journal of Engineering Innovation & Research*. 4(2).

Gladence, Y.O., & Brumancia, Y.E. (2020). *A Smart Home Design Based on Ethernet* (Acad J. Nawroz Univ) vol 6 no 3 pp 59–63

Govindraj, & Abubakar, (2021) *IoT Based Smart Home Using Blynk Framework* (Zerone Sch) vol 1 no 1 pp 26–30

Gunawan, Yaldi, & Kartiwi (2019). Design and Implementation of Low-Cost Home Security System using GSM Network. *International Journal of Scientific & Engineering Research.*

Hamed, J Sharmad Pasha, Dzhink (2021), Based Sensing and Monitoring System for IoT with MATLAB Analysisdz, IJNTR, Vol.2.

Lartigue,. Pradeep Kumar (2014), Arduino Based Wireless Intrusion Detection Using IR Sensor and GSM. *International Journal of Computer Science and Mobile Computing. 2(5): 417-424.*

Mehmood, & Kim, (2019), *An Integrated Approach Towards Designing an Embedded Wireless Monitoring and Access Control System Using RFID and MMS Technologies* pp 182–188

Montaser N. Ramadan, Mohammad A. Al-Khedher. Intelligent Anti-Theft and Tracking System for Automobiles. *International Journal of Machine Learning and Computing. 2012; 2(1).*

Oguntunde, Ojo, Okagbue, & Oguntunde (2018), Home Automation Using Internet of Things' IRJET Vol. 2, Issue no.3.

Prathaban, Thean, & Sazali, (2019), Method and Device to Communicate via SMS after a Security Intrusion. *1st International Conference on Sensing Technology. Palmerston North, New Zealand.*

Sarijari, Rashid, Rahim & Mahalin, (2021), Based Switching Using xMATLABdz, IJIREEICE, Vol.2

Singh. S.Boopathi, F.Parvez Ahmed, S.Thulasi Ram, M.Jagadeeshraja. Embedded Based Vehicle Speed Control System Using Wireless Technology. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. 2014; 2(8).*

Sriskanthan, Tan & Karande, (2020), Time Sensor Acquisition interfacing using MATLABdz, IEEE.

Wu S (2017), Saraladevi. B. Optimized Locking and Unlocking a System Using Arduino. *International Journal of Innovative Research in Computer and Communication Engineering. 2(11).*

Xiaodong, W.U. & Jie, X.U (2022), Embedded Based Vehicle Speed Control System Using Wireless Technology. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. 2(8).*